ExamLabs

NSE4 Fortinet Network Security Expert 4 Written

Study Guide

Exam NSE4

Table of Contents

Introduction to FortiGate Infrastructure Part-II picks up right where Part-I left off with Chapter 5. Part-I of the series focused on taking someone with basic computer networking knowledge and bringing them up to speed with basic FortiGate functions. Part-II builds on all the basic concepts by stepping into more advanced technologies FortiOS has to offer.

The NSE4 blueprint topics are logically separated into two sections, Infrastructure and Security. The purpose of this segregation of material is to build your skillset up layer by layer because you will not be able to understand DPI Web Filtering without first understanding basic FortiOS routing and the Session table functions. A common misconception is that there are two exams for the NSE4; this is false. You only need to pass one test to become NSE4 certified.

The feedback I received back from Introduction to FortiGate Part-II was mostly positive. People from around the world reached out to me to discuss the book's content and ask questions. I really felt a lot of appreciation from certain folks. I could tell other folks that already have FortiGate experience was a little frustrated with the book because it was too basic. With Part-II of this NSE4 study guide series, I hope to satisfy both sides of people who already have some FortiGate experience but looking to increase their skillset and folks who are new to FortiGate that only have the knowledge provided in Part-I. I'm confident that even the most experienced FortiGate engineers will learn something new after reading this book. I'm also confident that I will not lose new folks as I walk through the various topics discussed in this book.

Infrastructure - The basic underlying framework or features of a system or organization.

I recommended in Part-I of this NSE4 study guide series to have a lab because I feel like real hands-on experience is critical for understanding new technologies. I took this a step further in Part-II by providing detailed instructions on setting up a GNS3 lab with FortiOS VM. I urge you to take time and set up this lab before you start working your way through this book because as I discuss these various technologies, I hope you will be configuring FortiOS inline with me!

FortiOS is a fast-moving technology with constant updates and new features. Fortinet is one of the most innovative companies globally. It is honestly hard to keep up with all the changes, so I decided to base Part-II on 6.4, the latest MR. Once all books of this NSE4 study guide series are complete, one of my goals is to go back and upgrade all the content to the latest MR at that point in time. So as I release new books, they will be based on the latest MR regardless. With that being said, most folks do not run the latest MR in production; an N-1 method is more common. Essentially, this means operating one MR behind the latest. Using an N-1 MR method allows Fortinet to work major software defects out of new MR code bases. From what I've seen in my tenure working with Fortinet products and customers, a new MR production code base will not be deployed until at least the 4th patch within an MR. Note, this does not always hold true for engineering teams who aggressively certify Fortinet products to obtain the features they want for their deployments.

Infrastructure Part-II Chapter Overview

Part-II of the NSE4 study guide series has seven chapters and build off what you learned in Part-I. Here is the complete list of Chapters in this book:

Part-II Chapter 5 | VDOMs and Session Helpers

Chapter five starts off with reviewing Virtual Domains (VDOM) technology on FortiOS, a feature to segregate a single FortiGate into virtual firewalls. These virtual firewalls are autonomous from each other but share global settings. Chapter five also reviews Session Helper technology. Session Helpers are a new concept to many network engineers who only work with layer-2/layer-3 routers and switches. FortiGate is a stateful device, and therefore Sessions Helpers will always be a factor when working with protocols like FTP, SIP, or RTP.

Part-II Chapter 6 | High Availability (HA)

In chapter six, we begin our journey into FortiGate High Availability (HA) technologies. HA is a major item for modern networks accounting for hardware failures to maintain availability for countless network services. The argument is not if hardware will fail but when. FortiGate HA provides businesses the right tools to handle hardware failures gracefully.

Part-II Chapter 7 | Logging and Monitoring

In chapter seven, we step into the fundamental lifeline of any successful Security Operations Center (SoC), the log. FortiOS has robust logging around many different features. This chapter reviews how to configure logging and provides details around certain specific FortiOS logging features administrators need to account for. Lastly, in this chapter, various monitoring features

are discussed. FortiGate provides many monitoring tools to gain insight into what is going on within your network.

Part-II Chapter 8 | IPsec VPN

Chapter eight might be my favorite chapter in Part-II of this NSE4 study series. I have always loved working with IPsec, and this chapter provided us the opportunity to deep dive into the technology. After reading this chapter and knowing true, you will be confident in how IPsec works and how to implement it on FortiGate!

Part-II Chapter 9 | SSL VPN

Chapter nine focuses on TLS technology and how FortiGate uses this technology to create SSL-VPN for remote users! By the end of this chapter, you will feel confident in how TLS works and how to configure and manage SSL-VPN features on FortiOS.

Part-II Chapter 10 | SD-WAN

Chapter ten is where we get to the good stuff, SD-WAN. Within this chapter, we unmask this magical technology that focuses on dynamic best path application routing. By the end of this chapter, you will have a great foundation in FortiOS SD-WAN to build on.

Part-II Chapter 11 | Diagnostics and Troubleshooting

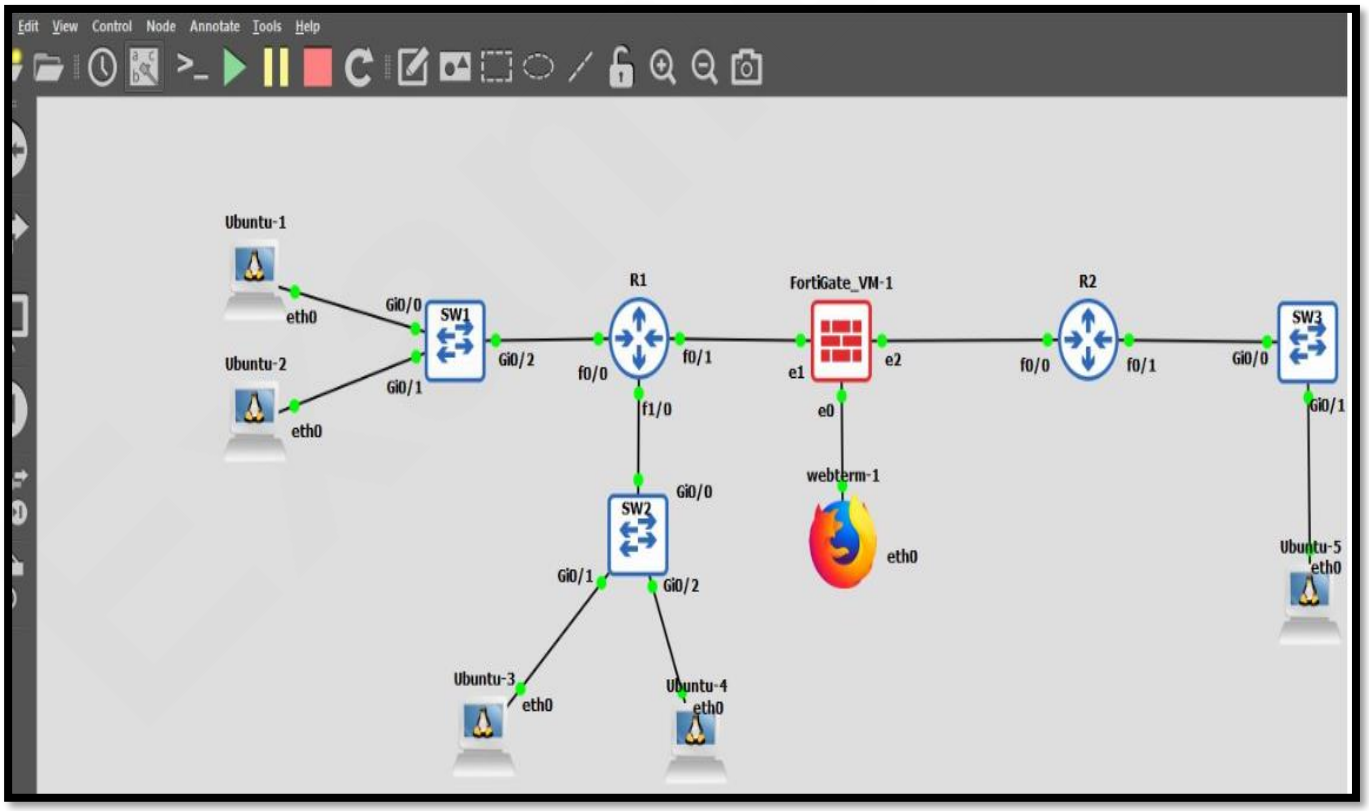
Chapter eleven, the last chapter of the book we focus on troubleshooting methodologies. We walk through various troubleshooting steps and methods, starting with the FortiGate system health. This chapter also touches on troubleshooting methods for networking, VPNs, HA, and SD-WAN.

FortiOS Lab Setup Guide

Not everyone has the cash to spend on purchasing a lab FortiGate device, but this doesn't mean there are no other avenues to obtain hands-on experience!

The purpose of this lab setup guide is to provide you an environment to practice what is discussed throughout the course of this book. Fortinet allows individuals to download a trial version of the FortiGate VM; note that the temporary license is only valid for 15 days. In this section, we walk through the steps to implement a virtualized network with FortiOS at the center. Please note that this is not an all-inclusive guide, such topics as how to navigate GNS3 and how to disable Hyper-V are not included. If you are experiencing any issues with the platforms demonstrated in this guide, I would suggest visiting the vendor forums or documentation. We will be using the following products in this lab setup guide:

- VirtualBox version 6.1.14 – This is what we will use as our hypervisor. A hypervisor enables us to run multiple virtual machines on our physical host and share our host's resources. Please note that additional host configuration may be needed.
- GNS3 version 2.2.14 – This is what we will use as our network simulator. GNS3 comes fitted with many tools such as Wireshark and can be utilized with the GNS3 VM to provide faster appliance deployments.



In addition to the platforms listed above, we will also be using several virtual machine images. This guide will document where to download these images and how to incorporate them into GNS3. We will be using the following software

- Cisco ISOv and Cisco ISOvl2 – These are the Cisco images we will use in the lab to simulate routers and switches. Cisco allows you to download these images, but you must purchase a Cisco VIRL license. There are other vendor router and switch images that are freely available to the public, as well.
- GNS3 VM version 2.2.14 – This is a Linux-based virtual machine that runs a GNS3 server; this allows us to run QEMU and KVM images from this server vs. our host machine. Windows host can have difficulties running KVM images.
- Fortinet VM64 KVM v6 build1778 – We will need to use the KVM version for this lab.
- Webterm – This is a GNS3 appliance that can be found from the GNS3 marketplace; it is free to use and will be our method to reach the FortiGate GUI.

Note the software versions for this lab because, as with any technology, things change. I believe this lab will continue to serve as a baseline and starting point for folks that wish to obtain hands-on experience with FortiOS.

Step 1: Install VirtualBox

- Visit ww.virtualbox.org
- Go to downloads and download the VirtualBox package for your platform.
- Run the VirtualBox .exe file.
- Proceed through the installation prompts typical install will be:
  - Click **Next** on the first three pages
  - Click **Yes** when prompted
  - Click **install** when prompted
  - Click **Yes** when prompted
- After VirtualBox has been installed, move on to step 2.

Step 2: Install GNS3

- Visit https://www.gns3.com/software/download
- Select the installer for your platform and click download.
- Once the download has been completed, run the .exe file.
- The GNS3 installation window will display a welcome message. Click **Next** to start the install.
- The next screen will display the License Agreement. Click, **I Agree** to proceed.
- Choose a start menu folder. I use the default “GNS3”.
- Next, you will be prompted to choose components to install with GNS3. These include Wireshark, Dynamips, QEMU, and so on. I will keep the preselected defaults and click **Next**.

- Select an installation folder or keep the default and click **install**.
- During the installation phase, if you have selected any third-party tools during the "Choose Components" step, they will be installed now. You will be prompted to accept the license agreement of third-party tools. Npcap will prompt you for installation options; make sure the following are selected:
    - Automatically start the Npcap driver at boot time
    - Support loopback traffic ("Npcap Loopback Adapter" will be created)
    - Support raw 802.11 traffic (and monitor mode) for wireless adapters
    - Support 802.1Q VLAN tag when capturing and sending data
- Click **Next** to install Npcap, then click finished once Npcap has finished installing.
- After GNS3 finishes installing, click **Next,** and you will be offered a free license of Solarwinds Standard Toolset. This is not required for the Fortigate lab; you can either download it or select no and click **Next**.
- At this point, GNS3 will be installed on your system; click Finish to close the GNS3 installation wizard.

Step 3: Install GNS3 VM

Before moving to this stage, VirtualBox and GNS3 need to be installed on your PC. Please note that for best performance, GNS3 and GNS3 VM need to be running the same version. If you have downloaded GNS3 in the past but not the VM, you might need to update your current GNS3 install. In the example, GNS3 2.2.16 will need GNS3 VM version 2.2.16 for optimal performance.

- Navigate to https://www.gns3.com/software/download-vm. Click the download link beside VirtualBox.
- Once downloaded, you need to extract the compressed file to the folder of your choosing.
- Next, we will need to import the gns3 VM.ova image into VirtualBox.
    - Open VirtualBox and select **New**
    - Enter the following information:
        - Name: GNS3 VM
        - Type: Other
        - Version: Other/Unknown (64-bit)
    - Click **Continue.**
    - Select the amount of memory to assign to this VM (you want to remain with in the green area of the slider) and click **Continue**.
    - VirtualBox will then prompt you for "Appliance to Import", select the gns vm.ova that we extracted earlier, and click **Continue**.
    - Next, set the appliance settings as needed; the defaults in our case will be fine. Then select **Import**.
- Next (once the import completes), we will need to configure the network adaptor for both VirtualBox and the GNS3 VM.

- Go to VirtualBox and select Preferences, then **Network**
- Here select the **Host-only Networks** tab
- Click the plus symbol on the right-hand-side and enter an IP and subnet mask for this adapter. You can use the automatically assigned IP from your system if you choose to do so, and click done once complete.
- Next right click on the GNS3 VM and select **Settings**
- Navigate to the **Network** menu and set Adapter 1 to **Enable** and attach it to **Host-only Adaptor**
- Select **vboxnet0** from the dropdown menu and click **OK**

Step 4: Configure GNS3

In this step, we will be configuring GNS3 to use the GNS3 VM, and we will be importing appliances to run our Fortigate lab.

- First, we will need to configure GNS3 to run using the GNS3 VM.
  - Run GNS3 and the Setup Wizard should launch automatically; if not, click help from the GNS3 menu and click Setup Wizard.
  - Select **Run modern IOS** and hit **NEXT.**
  - On this screen, you will be prompted to configure the local server, choose 127.0.0.1 from the menu (port should be 3080 TCP), and hit **NEXT**.
  - You will reach a screen that says "Local server status" with "Connection to local server successful" click **NEXT**. If you receive a warning that says "VirtualBox doesn't support nested virtualization", click **OK**.
  - The next screen will display, "In order to run the GNS3 VM, you must first have VMware or VirtualBox installed, and the GNS3 VM.ova imported with one of these software". Select VirtualBox and select the name of the GNS3 VM that we configured in VirtualBox (it should be auto-detected, make sure the VM is running). Assign the desired amount of vCPU cores and RAM, then click **Next**
  - The next page will display a summary. Click **Finish**.
  - GNS3 should now be configured to run using the GNS3 VM

- Next, we will need to import appliances to build our network topology. Remember that if you choose to use Cisco images, you will need a Cisco VIRL license (this method will work with other vendor images as well, some of these can be obtained for free from the vendor). I tend to use cisco-iosvl2 for network switches and cisco-iosv for network routers.
  - From GNS3 main view, click **File** from the toolbar, then select **Import appliance**.
  - Navigate to your **Downloads** folder (or destination where the images are stored) and click to open.
  - You will be prompted with a screen that says, "Please choose a server type to install the appliance", make sure that you select "install the appliance on the GNS3 VM (recommended)" and click **Next**.

- The next screen will display “Qemu settings”, make sure that **/user/bin/qemu-system-x86_64** is selected and click **Next**.
- The next screen will display the “Required Files”, on this page, you will need to select the appliance version that you wish to install. The status bar will show “Missing files”.
- Select the version of the VM that you wish to install and click **Import**. (The import option assumes that you already have the necessary file downloaded if GNS3 is unable to locate the file select **download**. This will open a browser window with the associate website to download the file.)
- After clicking **Import** (and after downloading the required file), a window will open, allowing you to browse to the file location of the image/virtual disk image for the device you are importing. Click **Open**.
- Next, GNS3 will check the md5 checksum and file size versus the .gnsa template; if the values match gns3 will upload a copy of that file to the GNS3 VM.
- In the “Required files” window, the status of the uploaded VM will change from “Missing” to “Ready to install”. Select the version of the uploaded VM and click **Next**.
- The next screen will display “Usage” and will display the default settings. Click **Finish**.
- Finally, you will be prompted that the appliance has been successfully installed. Click **Ok** to exit.
- You can now click the **Browse all Devices** options from the left menu pane to drag and drop the newly created appliance into your topology.

- Now we are ready to install the FortiGate KVM virtual firewall. As previously noted, you will need to visit the Fortinet support portal (https://support.fortinet.com) and register an account. You will navigate to **Downloads>VM Images>FortiGate** and select **KVM** as the platform, then just download the image.
  - Once you have downloaded the FortiGate KVM image, the file will need to be extracted. Simply right-click on the .zip file and click extract. The extracted file will be fortios.qcow2 as this is a QEMU image.
  - Next, open up GNS3 and navigate to **Edit>Preferences>QEMU>Qemu VMs** and click on **New**.
  - The “New QEMU VM template” window will be displayed; go ahead and name your FortiGate VM and click **Next**.
  - On this screen, you will need to assign RAM to the FortiGate; with the default 15-day license, a Fortinet VM only supports 1 CPU core and 1024 MB of RAM. Set the RAM to 1024 MB and click **Next**.
  - This screen will ask you to select a console type; for this demonstration, we will select **Telnet** and click **Next**.
  - This screen will ask you to “Please choose a base disk image for your virtual machine”, this is the fortios.qcow2 image that we downloaded earlier. Click **Browse..** and navigate to the file location of the .qcow2 image. Click **Finish**.

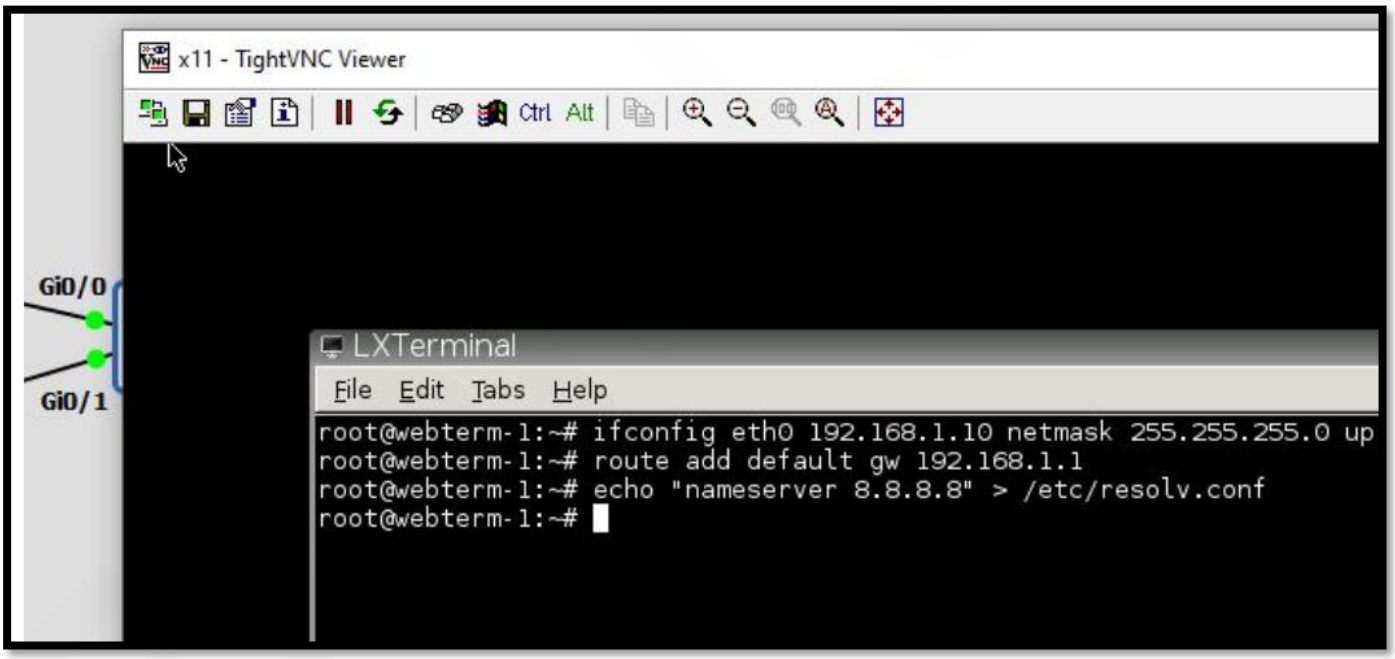
- You can customize your FortiGate VM further by clicking **Edit** from the GNS3 toolbar then selecting **Preferences**. Navigate to **QEMU VMs** and select the FortiGate VM and select **Edit**. Here you can configure the network adapter count, as well as interface type etc.

Step 5: Base FortiGate Configuration

In this step, we will be doing a basic network configuration for the FortiGate VM as well as installing Webterm to provide a web browser to log into the FortiGate VM GUI.

- Now that you have successfully created the FortiGate appliance, let's put a basic configuration on the device so that we can access the web GUI.
  - Click on all devices from the left GNS3 toolbar and select the FortiGate. Drag and drop the firewall into the GNS3 project area.
  - Right-click on the FortiGate and click on the start option; this will boot the device and open a console window. If the console window does not open automatically, right-click on the device and select console.
  - Once the device finishes booting, the console will prompt you to log in. The default username is admin, and the password is left blank.
  - FortiOS will now prompt you to change the admin password, change the password, and remember the password as you will use it to log into the GUI.
  - Now we will configure interface ethernet1/1 with an IP address and necessary services.
  - Enter the following console commands:
    - config system interface
    - edit port1
    - set mode static
    - set ip 192.168.1.1 255.255.255.0
    - set allowaccess https http ping ssh
    - end
  - At this point, you will be ready to install Webterm and access the web-based GUI.
- Webterm is a lightweight Linux-based docker container that includes a Firefox web browser; the following steps show how to download the appliance and install in GNS3.
  - First, browse to https://www.gns3.com and select marketplace, and search the marketplace for webterm.
  - Click the download button for webterm.
  - Once the download finishes, open up GNS3 and select **file>import appliance>** and select the webterm.gns3a image from your downloads folder and click open.
  - Select to install the appliance on the GNS3 VM and click **Next**.
  - Click **Finish** on the next screen, and Webterm will now be available to use in GNS3.

- Now we will configure Webterm with an IP address and connect the Webterm docker to our FortiGate firewall.
    - Click on all devices from the left GNS3 toolbar, drag and drop Webterm into the GNS3 project window.
    - Right-click on Webterm and select start, then double click on the device to bring up the TightVNC Viewer window.
    - A Firefox browser window will be displayed by default; minimize this window.
    - Left-click inside the TightVNC Viewer window to display a list of options and select **Terminal**. This action will open a Linux shell.
    - Enter the following commands to set the network for the Webterm docker. Please note that the IP address you assign Webterm will need to be in the same subnet as the recently created FortiGate VM.
        - ifconfig eth0 192.168.1.50 netmask 255.255.255.0 up
        - route add default gw 192.168.1.1
        - echo “nameserver 1.1.1.1” > /etc/resolv.conf
        - to verify type ifconfig



- Next, we will need to connect the Webterm docker container to the FortiGate VM via ethernet and log into the FortiGate http GUI.
    - From the GNS3 left toolbar, click add a link.
    - Click on the Webterm docker and select eth0.
    - Now click on the FortiGate VM and select eth0. Please note that in the above steps, we configured port1 on the FortiGate CLI; there is a naming offset in GNS3. **port1 = eth0**.

- Now click on Webterm to open the TightVNC Viewer. Mozilla Firefox should be displayed by default; if it is not, left-click and select **Applications>Mozilla Firefox**.
- Type http://192.168.1.1 and hit **enter**.
- You will reach the GUI login landing page, enter admin as the username and enter the password you configured in the FortiGate CLI earlier.
- At this point, you can now configure the FortiGate from the GUI and practice different scenarios in a lab setting.

Lab Setup Summary

Alright, folks, that's it! At this point, you should have a fully operational FortiOS lab! Nice work! Now we are ready to start working our way through chapter five! Let's get to it!